11-27-00

A

FISH & RICHARDSON P.C.

4350 La Jolla Village Drive
Suite 500
San Diego, California
92122

Telephone
858 678-5070

Facsimile
858 678-5099

Web Site
www.fr.com

Frederick P. Fish
1855-1930

W.K. Richardson
1859-1951

November 22, 2000

Attorney Docket No.: 10559/250001/P8899

Box Patent Application
Commissioner for Patents
Washington, DC 20231

Presented for filing is a new original patent application of:

Applicant: CARY A. JARDIN, ERIC VARSANYI, PHIL J. DUCLOS AND VINCENT M. PADUA

Title: LINK-LOCK DEVICE AND METHOD OF MONITORING AND CONTROLLING A LINK FOR FAILURES AND INTRUSIONS

FR

BOSTON
DALLAS
DELAWARE
NEW YORK
SAN DIEGO
SILICON VALLEY
TWIN CITIES
WASHINGTON, DC

Enclosed are the following papers, including those required to receive a filing date under 37 CFR §1.53(b):

	Pages
Specification	6
Claims	4
Abstract	1
Declaration	5
Drawing(s)	4

Enclosures:

— Assignment cover sheet and an assignment, 5 pages, and a separate $40 fee.
— Postcard.

CERTIFICATE OF MAILING BY EXPRESS MAIL

Express Mail Label No. EL558603198US

I hereby certify under 37 CFR §1.10 that this correspondence is being deposited with the United States Postal Service as Express Mail Post Office to Addressee with sufficient postage on the date indicated below and is addressed to the Commissioner for Patents, Washington, D.C. 20231.

November 22, 2000
Date of Deposit

Signature

Derek Norwood
Typed or Printed Name of Person Signing Certificate

18 total claims, 4 independent.

Basic filing fee	$710
Total claims in excess of 20 times $18	$0
Independent claims in excess of 3 times $80	$80
Fee for multiple dependent claims	$0
Total filing fee:	$790

A check for the filing fee is enclosed. Please apply any other required fees or any credits to deposit account 06-1050, referencing the attorney docket number shown above.

If this application is found to be incomplete, or if a telephone conference would otherwise be helpful, please call the undersigned at (858) 678-5070.

Kindly acknowledge receipt of this application by returning the enclosed postcard.

Please send all correspondence to:

SCOTT C. HARRIS
Fish & Richardson P.C.
4350 La Jolla Village Drive, Suite 500
San Diego, CA 92122

Respectfully submitted,

Scott C. Harris
Reg. No. 32,030
Enclosures
SCH/nsg
10079914.doc

Attorney's Docket No.: 10559/250001 / P8899

APPLICATION

FOR

UNITED STATES LETTERS PATENT

TITLE: LINK-LOCK DEVICE AND METHOD OF MONITORING AND CONTROLLING A LINK FOR FAILURES AND INTRUSIONS

APPLICANT: CARY A. JARDIN, ERIC VARSANYI, PHIL J. DUCLOS AND VINCENT M. PADUA

CERTIFICATE OF MAILING BY EXPRESS MAIL

Express Mail Label No. EL558603198US

I hereby certify under 37 CFR §1.10 that this correspondence is being deposited with the United States Postal Service as Express Mail Post Office to Addressee with sufficient postage on the date indicated below and is addressed to the Commissioner for Patents, Washington, D.C. 20231.

November 22, 2000
Date of Deposit

Signature

Derek Norwood
Typed or Printed Name of Person Signing Certificate

LINK-LOCK DEVICE AND METHOD OF MONITORING AND CONTROLLING A LINK FOR FAILURES AND INTRUSIONS

TECHNICAL FIELD

This invention relates to securing information across networks, and more particularly to monitoring and controlling a link between a network device and a computer for failures or intrusions.

BACKGROUND

The client/server model is often used to deliver information across a network. In this model, a client computer connects to a server on which information resides. The client computer may request the services of the server, such as delivering information. Other services may include searching for and sending back information, such as when a database on a network is queried.

A conceptual diagram of a computer network 100, such as the Internet, is illustrated in FIG. 1. The network 100 may comprise small computers 102-114 and large computers 120, 122, commonly used as servers. In general, small computers 102-114 are "personal computers" or workstations and are the sites at which a user operates the computer to

make requests for data from other computers or servers on the network 100.

A connection to the network 100 may be made through a network device 130-136 that provides an interface between the requesting computer (i.e. client) and the network infrastructure 140. The network device 130-136 may also be used to provide an interface between the network infrastructure 140 and the server 120, 122. The interface between the client 102-114, the server 120-122, and the network infrastructure 140 may be defined by a protocol referred to as the Hypertext Transfer Protocol (HTTP). The HTTP is the language that Web clients and servers use to communicate with each other. A secure version of this protocol, HTTP-S, is often used to provide communication between the network infrastructure 140 and the network device 130-136. However, the link between the network device 130-136 and the server 120-122, or the network device 130-136 and the small computer 102-114, is often configured in a non-secured mode.

DESCRIPTION OF DRAWINGS

These and other features and advantages of the invention will become more apparent upon reading the following detailed description and upon reference to the accompanying drawings.

Figure 1 is conceptual diagram of a computer network.

Figure 2 is a block diagram of a network system including a link lock system.

Figure 3 is a block diagram of a link lock system in accordance with an embodiment of the present disclosure.

FIG. 4 illustrates a method for monitoring and controlling a link for failures or intrusions according to an embodiment.

DETAILED DESCRIPTION

The present disclosure includes a link-lock system coupled to the network device to monitor and control the security mode of a link between the network device and the server or the client. The security mode of the link may be controlled in accordance with the status of the link. For example, if a link failure or intrusion is detected, the security mode of the link is maintained in a secured state rather than converted into a non-secured state.

An embodiment of a network 200 having the link-lock system 206 is illustrated in FIG. 2. The network 200 includes a network interface device 204 configured to interface with the network infrastructure 201 through a link 202 operating in a secured protocol (e.g. HTTP-S). The HTTP-S provides a variety of security mechanisms to HTTP clients and servers, providing the security service options appropriate to wide range of potential end uses.

The network 200 further includes a link-lock system 206 coupled to the network interface device 204. The link-lock system 206 monitors security status of the link 208 between the network interface device 206 and a computer used to connect to the network, such as the server or the client 210. In the illustrated embodiment of FIG. 2, when the link-lock system 206 determines that a link failure or intrusion is detected, the security protocol of the link 208 is maintained in an HTTP-S mode rather than converted into an HTTP mode. The link failure or intrusion may include physical tampering or alteration of any part of the link 208 between the network interface device 204 and the server/client 210. The failure or intrusion may also include software attack or modification of the link 208 from external sources.

A block diagram of the link-lock system 206 in accordance with an embodiment of the present disclosure is

shown in FIG. 3. The link-lock system 206 includes a bus monitor 300, a security switch 302, an encryption/decryption element 304, and a controller 306. The link-lock system 206 may also maintain a protocol encryption element 308 on the server/client 210.

The security switch 302 receives data from the network interface device 204 or the server/client 210. In the illustrated embodiment, the security switch 302 commands the encryption/decryption element 304 to convert the received data from a secured protocol to a non-secured protocol, when the data is received from a network link 310 and is placed onto the link 208. The security switch 302 may command the encryption/decryption element 304 to convert the received data from a non-secured protocol to a secured protocol, when the data is received from the link 208 and is placed onto the network link 310. The converted data is then sent to the server/client 210 or the network interface device 204 using an appropriate protocol.

The bus monitor 300 monitors the link 208 for possible link failure or intrusion. When a link failure or intrusion is detected on the link 208, the bus monitor 300 notifies the controller 306. The controller 306, upon receipt of the link failure, directs the security switch 302 to keep the link 208 in a secured protocol mode. The controller 306 may also direct the protocol encryption element 308 in the

server/client 210 to convert the data being placed on the link 208 using a secured protocol. In some embodiments, the functions of the security switch 302, the bus monitor 300, and the controller 306 may be combined into a single element.

FIG. 4 illustrates a method for monitoring and controlling a link for failures or intrusions. The method includes monitoring the link between a network device and a server/client, at 400. When failures or intrusions are detected on the link, at 402, the link is directed to use a secured protocol at 404. Data sent across this link remains in a secured protocol mode until a network manager determines that the failures or intrusions have been corrected at 406.

Numerous variations and modifications of the invention will become readily apparent to those skilled in the art. Accordingly, the invention may be embodied in other specific forms without departing from its spirit or essential characteristics.

WHAT IS CLAIMED IS:

1. A link lock system for a network, comprising:

a computer;

a network interface device to provide the computer with access to the network;

a bus monitor to monitor a first link between the network interface device and the computer, where said bus monitor reports detected failures or intrusions; and

a security switch to switch the first link from a non-secured mode to a secured mode when a report of said detected failures or intrusions is received from the bus monitor.

2. The system of claim 1, wherein said computer is a server.

3. The system of claim 1, wherein the network operates in a secured mode using an HTTP-S protocol.

4. The system of claim 1, wherein said non-secured mode of the first link between the network device and the computer uses HTTP protocol.

5. The system of claim 4, wherein said secured mode of the first link between the network device and the computer uses HTTP-S protocol.

6. The system of claim 1, further comprising:

a controller that receives the report from the bus monitor and sends control signals to the network interface device, the security switch, and the computer.

7. The system of claim 6, further comprising:

an encryption element in the computer, where said encryption element converts data placed on said first link to a secured protocol when the control signal is received from said controller.

8. A system for a server, comprising:

an interface device to provide the server with access to a network; and

a controller to monitor a link between the interface device and the server, where said controller switches the link from a non-secured protocol to a secured protocol when failures or intrusions are detected on the link.

9. The system of claim 8, wherein the network is Internet, such that the non-secured protocol includes HTTP and the secured protocol includes HTTP-S.

10. The system of claim 8, wherein said controller sends a control signal to the server when failures or intrusions are detected on the link.

11. The system of claim 10, further comprising:

an encryption element in the server, where said encryption element converts data placed on said link by the server to a secured protocol when the control signal is received from said controller.

12. A method, comprising:

monitoring a link between a network device and a computer;

first directing the link to use a secured protocol when failures or intrusions are detected on the link; and

second directing the link to revert to a non-secured protocol when said detected failures or intrusions have been corrected.

13. The method of claim 12, wherein said non-secured protocol includes HTTP protocol.

14. The method of claim 12, wherein said secured protocol includes HTTP-S protocol.

15. The method of claim 12, wherein the computer is a server.

16. An apparatus comprising a machine-readable storage medium having executable instructions that enable the machine to:

monitor a link between a network device and a server;

first directing the link to use a secured protocol when failures or intrusions are detected on the link; and

second directing the link to revert to a non-secured protocol when said detected failures or intrusions have been corrected.

17. The apparatus of claim 16, wherein said non-secured protocol includes HTTP protocol.

18. The apparatus of claim 16, wherein said secured protocol includes HTTP-S protocol.

ABSTRACT

A link lock system for a network is disclosed. The system includes a computer, a network interface device, a bus monitor, and a security switch. The network interface device provides the computer with access to the network. The bus monitor monitors a link between the network interface device and the computer. The bus monitor reports detected failures or intrusions. The security switch switches the link from a non-secured mode to a secured mode when a report of said detected failures or intrusions is received from the bus monitor.

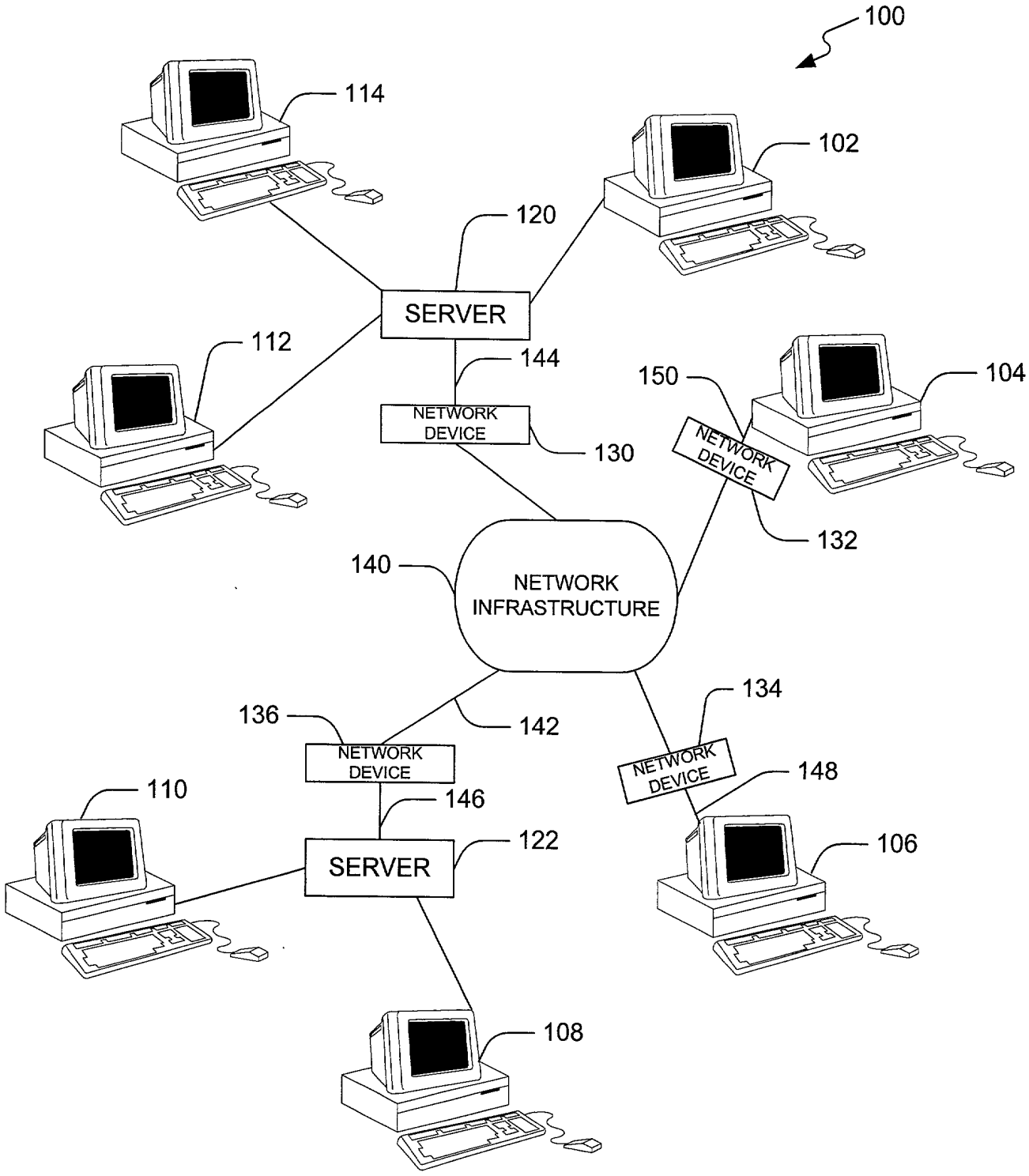

FIG. 1
(PRIOR ART)

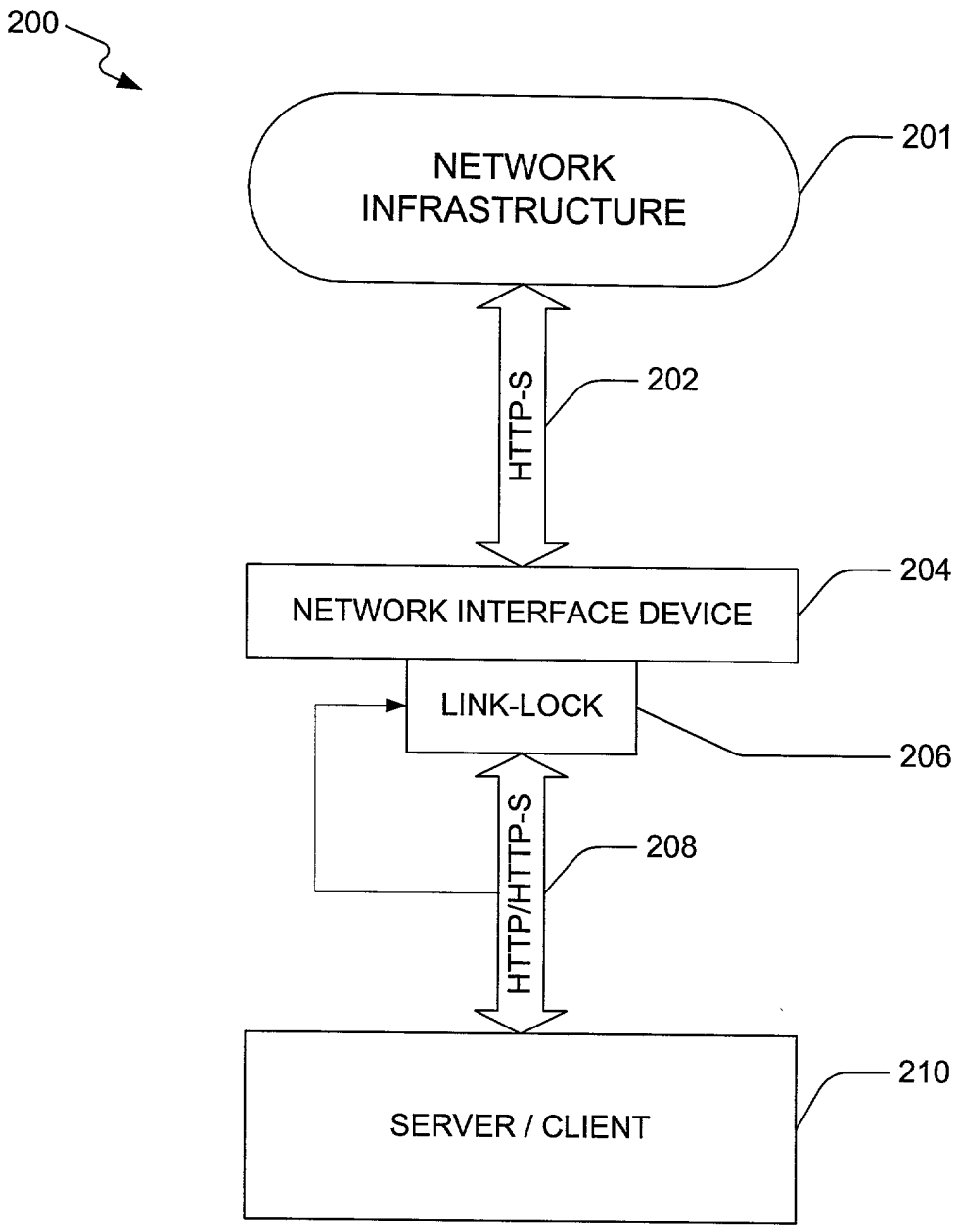
200
NETWORK INFRASTRUCTURE
201
HTTP-S
202
NETWORK INTERFACE DEVICE
204
LINK-LOCK
206
HTTP/HTTP-S
208
SERVER / CLIENT
210

FIG. 2

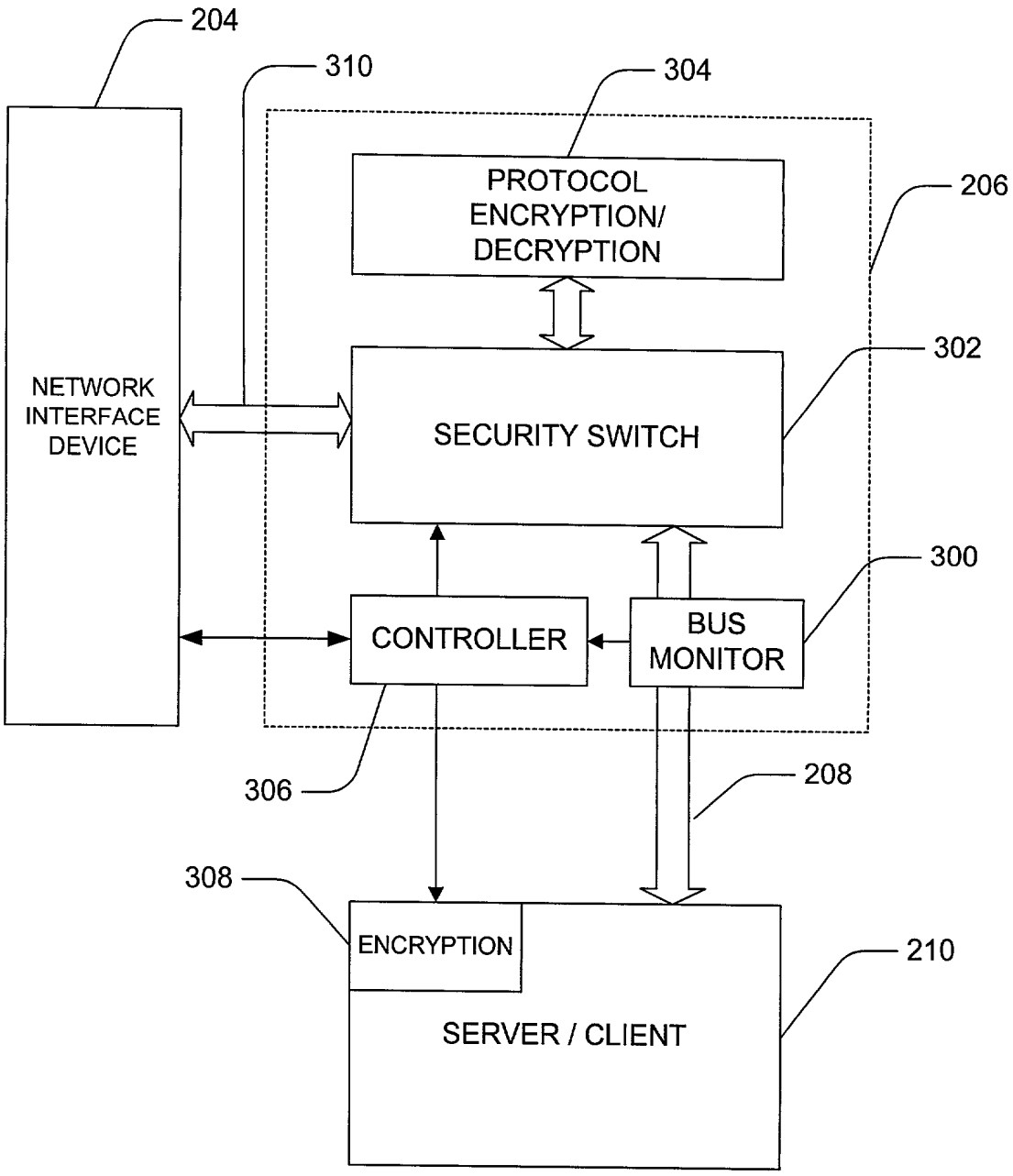
204
310
304
206
PROTOCOL
ENCRYPTION/
DECRYPTION
NETWORK
INTERFACE
DEVICE
302
SECURITY SWITCH
300
CONTROLLER
BUS
MONITOR
306
208
308
ENCRYPTION
210
SERVER / CLIENT

FIG. 3

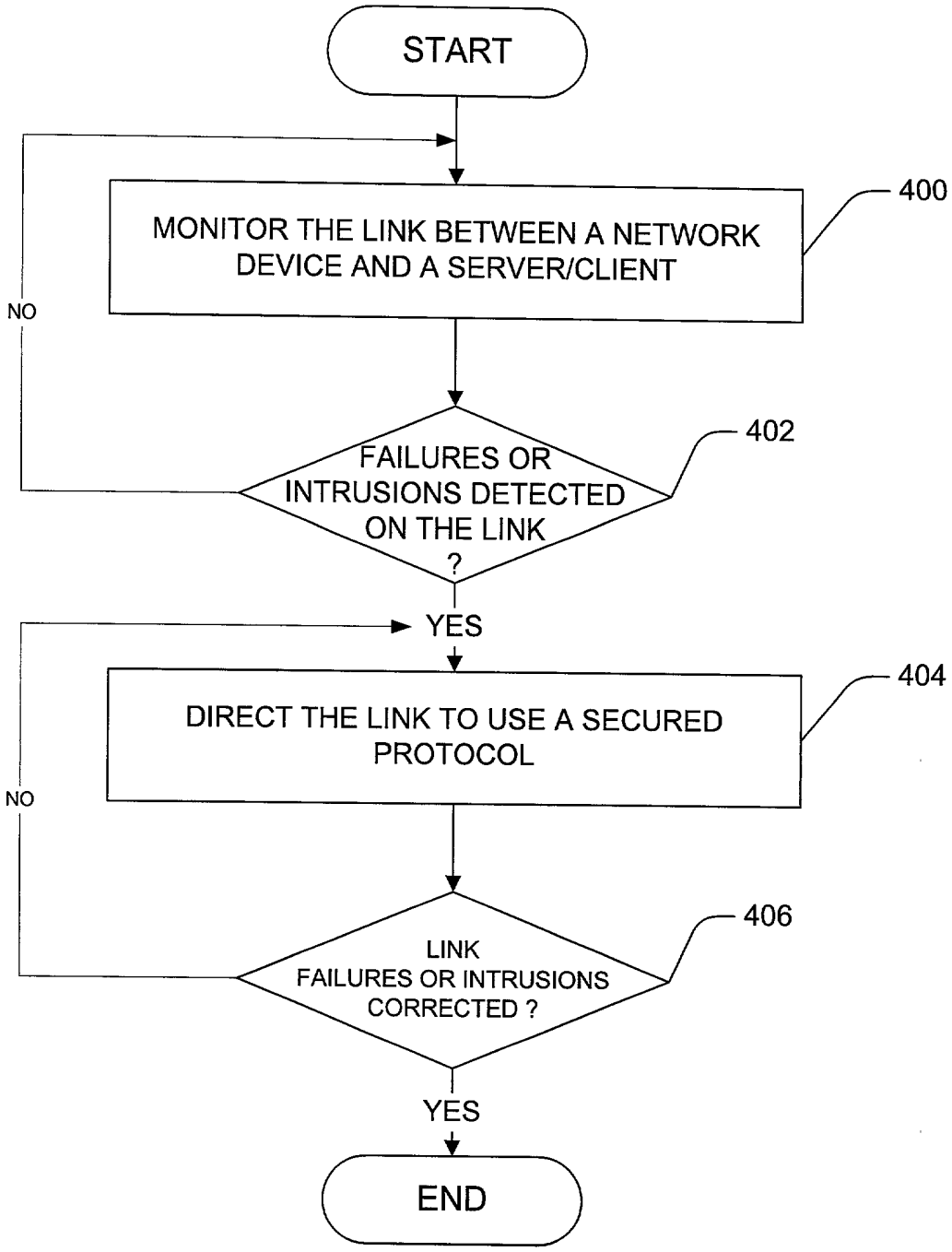
START
MONITOR THE LINK BETWEEN A NETWORK DEVICE AND A SERVER/CLIENT
400
NO
FAILURES OR INTRUSIONS DETECTED ON THE LINK ?
402
YES
DIRECT THE LINK TO USE A SECURED PROTOCOL
404
NO
LINK FAILURES OR INTRUSIONS CORRECTED ?
406
YES
END

FIG. 4

COMBINED DECLARATION AND POWER OF ATTORNEY

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below next to my name.

I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled LINK-LOCK DEVICE AND METHOD OF MONITORING AND CONTROLLING A LINK FOR FAILURES AND INTRUSIONS, the specification of which:

[X] is attached hereto.
[] was filed on _ as Application Serial No. _ and was amended on _____.
[] was described and claimed in PCT International Application No. _____ filed on _____ and as amended under PCT Article 19 on _____.

I hereby state that I have reviewed and understand the contents of the above-identified specification, including the claims, as amended by any amendment referred to above.

I acknowledge the duty to disclose all information I know to be material to patentability in accordance with Title 37, Code of Federal Regulations, §1.56.

I hereby claim the benefit under Title 35, United States Code, §119(e)(1) of any United States provisional application(s) listed below:

U.S. Serial No.	Filing Date	Status

I hereby claim the benefit under Title 35, United States Code, §120 of any United States application(s) listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States application in the manner provided by the first paragraph of Title 35, United States Code, §112, I acknowledge the duty to disclose all information I know to be material to patentability as defined in Title 37, Code of Federal Regulations, §1.56(a) which became available between the filing date of the prior application and the national or PCT international filing date of this application:

U.S. Serial No.	Filing Date	Status

I hereby claim foreign priority benefits under Title 35, United States Code, §119 of any foreign application(s) for patent or inventor's certificate or of any PCT international application(s) designating at least one country other than the United States of America listed below and have also identified below any foreign application for patent or inventor's certificate or any PCT international application(s) designating at least one country other than the United States of America filed by me on the same subject matter having a filing date before that of the application(s) of which priority is claimed:

Country	Application No.	Filing Date	Priority Claimed

Combined Declaration and Power of Attorney

I hereby appoint the following attorneys and/or agents to prosecute this application and to transact all business in the Patent and Trademark Office connected therewith:

Scott C. Harris, Reg. No. 32,030
David L. Feigenbaum, Reg. No. 30,378
Hans R. Troesch, Reg. No.36,950
Bing Ai, Reg. No. 43,312
Samuel L. Lee, Reg. No. 42,791
Frederick H. Rabin, Reg. No. 24,488
William J. Egan, III, Reg. No. 28,411
James T. Hagler, Reg.. No,. 40,631
John R. Wetherell, Jr., Reg. No. 31,678
Kenyon S. Jenckes, Reg. No. 41,873
Richard J. Anderson, Reg. No. 36,732
Samuel Borodach, Reg. No. 38,388

Address all telephone calls to SCOTT C. HARRIS at telephone number (858) 678-5070.

Address all correspondence to SCOTT C. HARRIS at:

FISH & RICHARDSON P.C.
PTO Customer No. 20985
4350 La Jolla Village Drive, Suite 500
San Diego, CA 92122

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patents issued thereon.

Full Name of Inventor: CARY A. JARDIN

Inventor's Signature: _____ Date: 11-17-00
Residence Address: 12662 Sabre View Cove
San Diego, CA 92128
Citizenship: U.S.
Post Office Address: 12662 Sabre View Cove
San Diego, CA 92128

Full Name of Inventor: ERIC VARSANYI

Inventor's Signature: _____ Date: _____
Residence Address: 4100 Ives Lane North
Plymouth, MN 55441
Citizenship: U.S.
Post Office Address: 4100 Ives Lane North
Plymouth, MN 55441

Combined Declaration and Power of Attorney

I hereby appoint the following attorneys and/or agents to prosecute this application and to transact all business in the Patent and Trademark Office connected therewith:

Scott C. Harris, Reg. No. 32,030
David L. Feigenbaum, Reg. No. 30,378
Hans R. Troesch, Reg. No.36,950
Bing Ai, Reg. No. 43,312
Samuel L. Lee, Reg. No. 42,791
Frederick H. Rabin, Reg. No. 24,488
William J. Egan, III, Reg. No. 28,411
James T. Hagler, Reg.. No,. 40,631
John R. Wetherell, Jr., Reg. No. 31,678
Kenyon S. Jenckes, Reg. No. 41,873
Richard J. Anderson, Reg. No. 36,732
Samuel Borodach, Reg. No. 38,388

Address all telephone calls to SCOTT C. HARRIS at telephone number (858) 678-5070.

Address all correspondence to SCOTT C. HARRIS at:

FISH & RICHARDSON P.C.
PTO Customer No. 20985
4350 La Jolla Village Drive, Suite 500
San Diego, CA 92122

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patents issued thereon.

Full Name of Inventor: CARY A. JARDIN

Inventor's Signature: _____ Date: _____
Residence Address: 12662 Sabre View Cove
San Diego, CA 92128
Citizenship: U.S.
Post Office Address: 12662 Sabre View Cove
San Diego, CA 92128

Full Name of Inventor: ERIC VARSANYI

Inventor's Signature: _____ Date: 11/23/2005
Residence Address: 4100 Ives Lane North
Plymouth, MN 55441
Citizenship: U.S.
Post Office Address: 4100 Ives Lane North
Plymouth, MN 55441

Attorney's Docket No.: 10559/250001/P8899

Combined Declaration and Power of Attorney

Full Name of Inventor: PHIL J. DUCLOS

Inventor's Signature: Philip J. Duclos Date: 11/16/00

Residence Address: 12968 Hillcrest Drive
Longmont, CO 80504

Citizenship: U.S.

Post Office Address: 12968 Hillcrest Drive
Longmont, CO 80504

Full Name of Inventor: VINCENT M. PADUA

Inventor's Signature: _____ Date: _____

Residence Address: 13912 Capewood Lane, #296
San Diego, CA 92128

Citizenship: U.S.

Post Office Address: 13912 Capewood Lane, #296
San Diego, CA 92128

Combined Declaration and Power of Attorney

Full Name of Inventor: PHIL J. DUCLOS

Inventor's Signature: _____ Date: _____

Residence Address: 12968 Hillcrest Drive
Longmont, CO 80504

Citizenship: U.S.

Post Office Address: 12968 Hillcrest Drive
Longmont, CO 80504

Full Name of Inventor: VINCENT M. PADUA

Inventor's Signature: _____ Date: 11.16.00

Residence Address: 13912 Capewood Lane, #296
San Diego, CA 92128

Citizenship: U.S.

Post Office Address: 13912 Capewood Lane, #296
San Diego, CA 92128